

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-186718

(43)Date of publication of application : 15.07.1997

(51)Int.Cl.

H04L 12/56

(21)Application number : 07-341984

(71)Applicant : FUJITSU LTD

(22)Date of filing : 28.12.1995

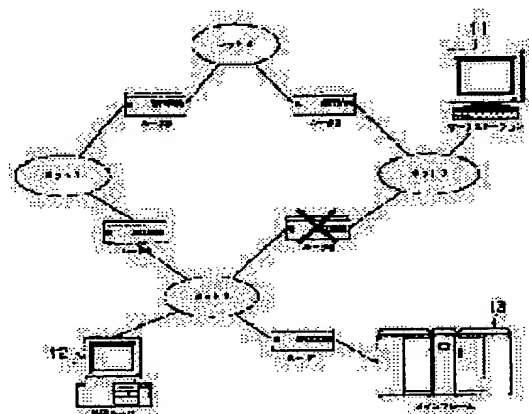
(72)Inventor : TANBA NAOTO

(54) PATH CONTROLLER CONTROLLING NETWORK PATH AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To allow the method to make countermeasure and restoration to a network fault by controlling automatically a path such as communication lines configured as a network.

SOLUTION: Each router in a computer network has a path table in which adjacent destination routers are registered for each communication. In the case of communication by a work station 11 via routers 4, 1 with a main frame 13, when the router 4 is defective, the router 4 reports a fault to adjacent routers 1, 2, 3. Each router receiving the notice excludes the router 4 to update the path table and other adjacent router is registered as a substitute router. Thus, a substitute path via routers 2, 5, 3, 1 is automatically set.



LEGAL STATUS

[Date of request for examination]

29.08.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3577151

[Date of registration]

16.07.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-186718

(43) 公開日 平成9年(1997)7月15日

(51) Int.Cl.⁶

H 0 4 L 12/56

識別記号

庁内整理番号

9466-5K

F I

H 0 4 L 11/20

技術表示箇所

1 0 2 D

審査請求 未請求 請求項の数13 O L (全 16 頁)

(21) 出願番号 特願平7-341984

(22) 出願日 平成7年(1995)12月28日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 丹波 直人

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74) 代理人 弁理士 大菅 義之 (外1名)

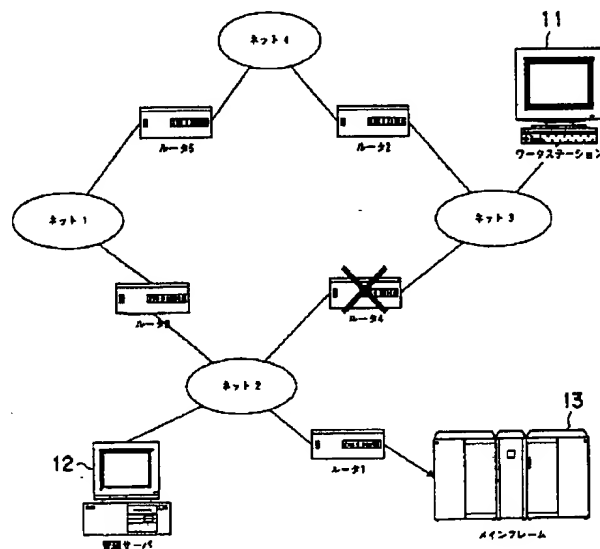
(54) 【発明の名称】 ネットワークの経路を制御する経路制御装置および方法

(57) 【要約】

【課題】 ネットワーク状に構成された通信路等の経路を自動的に制御して、ネットワーク障害に対する対処・復旧等を行うことが課題である。

【解決手段】 コンピュータ・ネットワーク内の各ルータは、それぞれの通信毎に隣接する送信先ルータを登録した経路表を保持している。ワークステーション11がルータ4、ルータ1を介してメインフレーム13と通信を行っている時、ルータ4が不調になると、ルータ4は隣接するルータ1、2、3に異常を通知する。通知を受けた各ルータは、ルータ4を除外して経路表の更新を行い、別の隣接ルータを代替ルータとして登録する。これにより、ルータ2、5、3、1を経由する代替経路が自動的に設定される。

コンピュータ・ネットワークを示す図



【特許請求の範囲】

【請求項1】 複数の経路を含む通信ネットワーク上に設けられ、通信制御のための経路情報を管理する情報処理装置において、

前記ネットワーク上の第1の経路に関する異常を検出する検出手段と、

前記第1の経路に異常が発生した時、前記ネットワーク上の他の情報処理装置に、該第1の経路に関する局所的な経路情報を更新するよう指示し、早めに代替となる第2の経路を探索させる指示手段とを備えることを特徴とする経路制御装置。

【請求項2】 前記指示手段は、前記他の情報処理装置のアドレス情報を連絡先として格納する緊急連絡表を保持することを特徴とする請求項1記載の経路制御装置。

【請求項3】 前記指示手段は、前記他の情報処理装置にエージェントプロセスを送付して、前記第2の経路を探索させることを特徴とする請求項1記載の経路制御装置。

【請求項4】 複数の経路を含む通信ネットワーク上に設けられ、通信制御のための経路情報を管理する情報処理装置において、

前記ネットワーク上の第1の経路に関する異常通知を受信する受信手段と、

前記異常通知に基づいて、前記第1の経路に関する局所的な経路情報を更新し、早めに代替となる第2の経路を探索する探索手段とを備えることを特徴とする経路制御装置。

【請求項5】 前記第2の経路が見つかった時、代替経路が設定されたことを他の情報処理装置に通知する通知手段をさらに備えることを特徴とする請求項4記載の経路制御装置。

【請求項6】 前記探索手段は、他の情報処理装置と経路情報を交換することにより、前記第1の経路に関する経路情報を更新することを特徴とする請求項4記載の経路制御装置。

【請求項7】 前記受信手段は、前記異常を知らせるエージェントプロセスを受信し、前記探索手段は、該エージェントプロセスが持っている前記第1の経路の識別情報を参照して、前記第2の経路を探索することを特徴とする請求項4記載の経路制御装置。

【請求項8】 前記第2の経路が見つかったかどうかを示す情報を前記エージェントプロセスに設定して、送信元の情報処理装置に送り返す通知手段をさらに備えることを特徴とする請求項7記載の経路制御装置。

【請求項9】 複数の経路を含むネットワークの経路情報を管理する情報処理装置において、前記ネットワークの局所的な経路情報を記憶する記憶手段と、

前記ネットワーク上の第1の経路に異常が発生した時、該異常が発生した場所の近傍の経路情報を変更して、早

めに代替となる第2の経路を探索する探索手段とを備えることを特徴とする経路制御装置。

【請求項10】 複数の経路を含む通信ネットワーク上に設けられた情報処理装置によって使用された時、前記ネットワーク上の第1の経路に関する異常を検出する機能と、

前記第1の経路に異常が発生した時、前記ネットワーク上の他の装置に、該第1の経路に関する局所的な経路情報を更新するよう指示し、早めに代替となる第2の経路を探索させる機能とを前記情報処理装置に行わせるための読み出し可能媒体。

【請求項11】 複数の経路を含む通信ネットワーク上に設けられた情報処理装置によって使用された時、前記ネットワーク上の第1の経路に関する異常通知を受信する機能と、

前記異常通知に基づいて、前記第1の経路に関する局所的な経路情報を更新し、早めに代替となる第2の経路を探索する機能とを前記情報処理装置に行わせるための読み出し可能媒体。

【請求項12】 複数の経路を含むネットワークの経路情報を管理する情報処理装置によって使用された時、前記ネットワークの局所的な経路情報を作成する機能と、

前記ネットワーク上の第1の経路に異常が発生した時、該異常が発生した場所の近傍の経路情報を変更して、早めに代替となる第2の経路を探索する機能とを前記情報処理装置に行わせるための読み出し可能媒体。

【請求項13】 複数の経路を含むネットワークの経路情報を管理する方法において、

前記ネットワークの局所的な経路情報を作成し、前記ネットワーク上の第1の経路に異常が発生した時、該異常が発生した場所の近傍の経路情報を変更して、早めに代替となる第2の経路を探索することを特徴とする経路制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク状に構成された通信路や交通路等の経路を動的に制御する経路制御装置およびその方法に関する。

【0002】

【従来の技術】近年、コンピュータ資源の分散化に伴って、複数の通信ネットワークを結合したグローバルなコンピュータ・ネットワークが構築されている。このような大規模なネットワークにおいては、円滑な通信環境を提供することがますます重要になっており、従来より経路情報をを用いた通信制御が行われている。

【0003】経路情報とは、ネットワークに送出されたデータの packets を、どのネットワークに転送するのか、転送するとしたらどこを中継するのかを判断するための基本となる重要な情報である。経路情報は、ネット

ワークを中継する機器（ゲートウェイ）の中で、経路表（ルーティング・テーブル）という形で保持されている。

【0004】経路表は、終点アドレスと、そこへデータの packets を届けるために中継すべき隣接ゲートウェイのアドレスの対になった表である。各ゲートウェイは、データの packets が届くたびに、経路表から次のゲートウェイのアドレスを求め、そのゲートウェイに packets を転送する。こうして、目的の場所へ packets が届けられる仕組みになっている。

【0005】経路情報は各ゲートウェイで保持されるが、その内容はネットワーク全体で一貫性をもって管理されなければならない。現在の大規模なネットワーク環境では、障害や工事、保守点検などは日常的に発生している。さらに、ネットワークに新たな機器や端末が接続されるなど、ネットワークの接続状態は常に変化している。この変化に伴って経路情報を更新しなければならないが、経路情報を人手で設定したり、どこかで全体を集中管理することは現実的に不可能である。

【0006】そこで、経路情報を保守・配付するためのプロトコルが決められており、ポピュラーなものとしては、RFC (Requests For Comments) 1058 に定められた RIP (Routing Information Protocol) が存在する。RIP はインターネットの IP プロトコルの経路制御に用いられているほか、Novell 社のネットワーク OS である Net Ware の IPX / SPX プロトコルや、Apple 社の Macintosh で採用されている Apple Talk プロトコルの経路制御にも、ほぼ同様の形式が用いられている。

【0007】

【発明が解決しようとする課題】しかしながら、上述した従来の経路情報制御には次のような問題がある。経路情報を保持・配付しているネットワーク機器に障害が発生した場合、その保持・配付作業にも障害が発生する。最悪の場合、経路情報の配布が停止し、ネットワーク全体の通信が停止状態になることもある。現状では、機器に自立的に復旧する能力が無いため、管理者が手作業で故障した機器を復旧するまで、ネットワークが混乱状態や停止状態のままになってしまう。

【0008】現状では、経路情報を 1 箇所で集中的に管理することはできず、また、それを人手で設定することもできない。このため、ネットワーク上の故障した機器を迂回して代替経路をすぐに確保したり、ネットワーク上の packets の流れを制限するといったことを自動的に行う有効な方法はない。

【0009】したがって、ネットワークが一時的に高負荷になった場合や、障害などでネットワークそのものがダウンした場合、現状では管理者が管理ツールや機器を用いて、手作業でネットワークの状況を調べて対処していることが多い。このとき、ネットワークは異常な状態にあるので、平常時であれば有効に動作する管理ツール

や管理機器であっても、ネットワーク上の異常通信の負荷などによってその動作が妨げられ、結果的に対処が遅れる可能性が高い。

【0010】本発明は、ネットワーク状に構成された通信路等の経路を自動的に制御して、ネットワーク障害に対する対処・復旧等を行う経路制御装置およびその方法を提供することを目的とする。

【0011】

【課題を解決するための手段】図 1 は、本発明の経路制御装置の原理図である。図 1 において、情報処理装置 1 および 4 は、複数の経路を含む通信ネットワーク上に設けられ、経路制御装置として動作する。

【0012】情報処理装置 1 は、検出手段 2 と指示手段 3 を備える。検出手段 2 は、上記ネットワーク上の第 1 の経路に関する異常を検出する。指示手段 3 は、第 1 の経路に異常が発生した時、上記ネットワーク上の他の情報処理装置 4 に、第 1 の経路に関する局所的な経路情報を更新するよう指示し、早めに代替となる第 2 の経路を探索させる。

【0013】第 1 の経路に関する異常とは、通信負荷の増大（輻湊）、通信障害、経路上の機器の故障、不正な通信など、通常の通信が妨げられる状態を指す。情報処理装置 1 の近くを経由する通信をモニタしている検出手段 2 がこのような異常を検出すると、それを指示手段 3 に伝える。

【0014】指示手段 3 は、第 1 の経路が完全に使えなくなる前にその代替となる第 2 の経路を探すよう、ネットワークを介して情報処理装置 4 に指示する。この指示を受けて、情報処理装置 4 は第 1 の経路に関する経路情報を更新し、代替経路があるかどうかを調べる。

【0015】経路情報としては、例えば RIP に基づく経路表が用いられる。経路表には、通信経路上のすべての機器の接続情報が記載されているわけではなく、例えば情報処理装置 4 から離れたある目標装置にデータを送る場合に、差し当たってどの隣接機器（ルータ等）に送ればよいかといった情報が格納される。したがって、経路情報は、情報処理装置 4 の近傍の局所的な送信先を記述している。

【0016】経路表を用いた場合、その情報を RIP に基づいてネットワーク上の隣接機器間で交換することにより、更新することができる。本発明では、情報処理装置 4 が指示手段 3 からの指示に従って、経路情報を更新する。

【0017】このとき、第 1 の経路に含まれる隣接機器を送信先からはずしておけば、別の隣接機器が自動的に新たな送信先として登録される可能性がある。このような代替送信先が見つければ、それを含む経路が代替経路となる。

【0018】情報処理装置 4 は、受信手段 5、探索手段 6、および記憶手段 7 を備える。受信手段 5 は、上記ネ

ットワーク上の第1の経路に関する異常通知を受信する。探索手段6は、その異常通知に基づいて、記憶手段7内に記憶された第1の経路に関する局所的な経路情報を更新し、早めに代替となる第2の経路を探索する。

【0019】受信手段5は、例えば情報処理装置1から第1の経路上に異常が発生したことを通知されると、それを探索手段6に伝える。これを受けて、探索手段6は、例えば上述の経路表に記述された経路情報をRIPに基づいて更新し、代替送信先を探す。そして、代替送信先が見つければ、それを第2の経路に関する経路情報として登録する。

【0020】また、情報処理装置4は、交通機関のネットワークなど、通信ネットワーク以外の任意のネットワークの経路情報を管理することもできる。この場合、情報処理装置4をネットワークから切り離して設けることができ、受信手段5は必ずしも必要ではない。記憶手段7は、そのネットワークの局所的な経路情報を記憶する。探索手段6は、ネットワーク上の第1の経路に異常が発生した時、該異常が発生した場所の近傍の経路情報を変更して、早めに代替となる第2の経路を探索する。

【0021】この場合の経路情報としても、通信ネットワークにおける経路表と同様に局所的な情報を用いる。例えば、ネットワーク上の各ノード毎に、目的地までの経路の情報として、隣接する次の移動先ノードを記憶しておく。そして、第1の経路に異常が発生した時、探索手段6が、その場所の近傍のいくつかのノードに対応する経路情報を更新して、代わりとなる移動先ノードを探す。そのような移動先ノードが見つければ、第2の経路に関する経路情報として登録される。

【0022】このような経路制御装置を用いれば、ネットワークが一時的に高負荷になった場合や、ネットワークそのものがダウンした場合などに、ネットワーク自身が自動的に迂回経路を設定することができる。管理者はネットワークの状況を調べて代替経路を設定する必要がなく、また、各経路の代替経路をあらかじめ登録しておく必要もない。

【0023】例えば、図1の情報処理装置1は、実施形態の図2におけるルータ4に対応し、情報処理装置4は、ルータ1、ルータ2、ルータ3に対応する。また、例えば、検出手段2は図7における通信ポート制御部42に対応し、指示手段3と探索手段6は制御エージェント部41に対応し、受信手段5は図11における通信ポート58に対応し、記憶手段7はメモリ57に対応する。

【0024】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。図2は、実施形態のコンピュータ・ネットワークを示している。図2のコンピュータ・ネットワークは、ネット1、ネット2、ネット3、ネット4の4つのネットワークを含む。ネット1

とネット2はルータ3を介して接続されており、ネット2とネット3はルータ4を介して接続されている。ネット3とネット4はルータ2を介して接続されており、ネット4とネット1はルータ5を介して接続されている。これらのルータは、ネットワーク間のゲートウェイの役割を果たしている。

【0025】また、ネット3にはワークステーション11が接続されており、ネット2には管理サーバ12が接続されている。さらに、ネット2にはルータ1を介してメインフレーム13が接続されている。このようなネットワークにおいて、ユーザがワークステーション11からメインフレーム13を利用しているとする。

【0026】現在ポピュラーに用いられているRIP等では、データパケットが終点に到達するまでに通過するゲートウェイの数(中継数)を基準にして経路の選択を行っている。例えば、ワークステーション11からメインフレーム13への通信経路としては、
ワークステーション11==ネット3==ルータ4==
ネット2==ルータ1==メインフレーム13
が採用される。

【0027】この状態で利用中にルータ4が不調になったとする。このとき、図2では、
ワークステーション11==ネット3==ルータ2==
ネット4==ルータ5==ネット1==ルータ3==
ネット2==ルータ1==メインフレーム13
という迂回経路が存在する。この場合、主としてルータ1、ルータ2、ルータ3、およびルータ4が経路制御装置の機能を果たし、この迂回経路を自動的に経路表に設定する。

【0028】各ルータは、それぞれの経路表のほかに障害発生時の通知先ルータを管理する緊急連絡表を保持しており、これを参照しながら異常通知を行う。通知を受けたルータは、通常の経路表更新時以外のタイミングで、RIPに従って他のルータと経路情報を交換し、自ルータの経路表を更新する。この結果、異常ルータに代わる新たなルータが経路表に登録されれば、それを代替経路として設定する。

【0029】例えば、不調になったルータ4は、ネットワーク上で隣接するルータ1、ルータ2、ルータ3を通知先として管理しており、これらの各ルータに異常を通知する。通知を受けた各ルータは、ルータ4を除外してRIPに基づいた経路表の更新を行い、次に中継数の少ない経路に属するルータを代替ルータとして登録する。

【0030】これにより、ルータ1の経路表にはルータ4の代わりにルータ3が登録され、ルータ2とルータ3の経路表にはルータ4の代わりにルータ5が登録される。ルータ5の経路表には、元々ルータ2とルータ3を結ぶ情報が設定されているので、上述のような迂回経路が自動的に確保されることになる。

【0031】代替経路が設定されたルータはそのことを

ルータ4に通知し、ルータ4は緊急連絡表内で、それらのルータに印を付けておく。これにより、代替経路が設定されたルータが、その設定に失敗したルータと区別される。また、ルータ4の経路表は更新されずに保存され、ルータ4の復旧時に再び使用される。

【0032】復旧時には、ルータ4は緊急連絡表を参照し、印の付けられたルータに復旧通知を行う。これを受けて、ルータ1、ルータ2、ルータ3は、それぞれの経路表を元の状態に再設定する。こうして、異常発生前のルータ4を経由する通信経路が再び使用可能となる。

【0033】上述のようなルータ間の経路制御情報の伝達は任意の通信処理により実現可能であるが、以下の実施形態では、一例としてリモートプログラミングに基づく言語であるテレスクリプト (Telescript) による方法を用いることにする。

【0034】テレスクリプトによるリモートプログラミングにおいては、データを保持するプロセスの一種であるエージェント (Agent) が用いられる。この場合には、各ユーザの監視要求情報を各エージェントに持たせることが可能であるため、複数のユーザの要求を独立に処理することができる。さらに、エージェントは自律的に機能して、処理が終了すれば自動的に消滅するため、不特定多数のユーザが利用するネットワーク上の処理に適している。

【0035】テレスクリプトによるリモートプログラミングについては、「リモートプログラミングの実施方法」(特願平6-179767、特開平7-182174)に詳述されているが、ここでその手法について説明する。

【0036】このリモートプログラミングは、複数の計算機システムを結ぶ通信ネットワーク上での処理を記述する方法の一種で、ネットワークを渡り歩く移動可能なプロセスであるエージェントと、エージェントが入ってくる固定プロセスであるプレイス (Place) により実現される。

【0037】図3は、プレイスの構成を示している。プレイスは、他のプロセスと識別可能なテレネーム (tele name) を持ち、任意有限個の子プロセスを持つことができる。また、プレイスは、自己および他のプロセスより参照可能な任意有限個のデータと、自己および他のプロセスより呼出し可能な任意有限個の手続きとを有する。

【0038】さらに、メインルーチンとして手続きliveを持ち、作成されたプレイスはliveを実行する。プレイスは、liveが実行されている間だけ存在し、liveが終了すると消滅する。プレイスが消滅すると、その子プロセスも終了し、消滅する。

【0039】図4は、エージェントの構成を示している。エージェントは、他のプロセスと識別可能なテレネームを持ち、あるプレイスの中の子プロセスとしてのみ存在する。また、エージェントは、自己および他のプロ

セスより参照可能な任意有限個のデータと、自己および他のプロセスより呼出し可能な任意有限個の手続きとを有する。

【0040】さらに、メインルーチンとして手続きliveを持ち、作成されたエージェントはliveを実行する。エージェントは、liveが実行されている間だけ存在し、liveが終了すると消滅する。エージェントの手続きliveの中でコマンドgoが実行されると、そのエージェントはネットワークを介して指定された行き先へ移動する。

【0041】図5は、コマンドgoによるオペレーションの例を示している。図5において、プレイス21内のエージェント22は、goの実行により、行き先のプレイス24を指定するデータであるチケット (Ticket) 23を得て、指定されたプレイス24に移動する。

【0042】このとき、エージェント22は、goによりliveの実行を一時中断し、保持したデータとともに凍結 (圧縮) され、バック化される。そして、チケット23に示されたプレイス24に送られ、プレイス24により受け入れをチェックされる。プレイス24に受け入れられると、その中に子プロセスとして置かれた後、解凍 (伸張) され、goの次のコマンドからliveの実行を再開する。

【0043】また、エージェントは、手続きliveの中で自己の置かれているプレイス内にある他のエージェントを求めるコマンドmeetを呼出すことができる。コマンドmeetの実行時には、エージェントは相手のエージェントを指定するデータであるペティション (Petition) を用いる。

【0044】図6は、コマンドmeetによるオペレーションの例を示している。図6において、プレイス31内のエージェント32は、コマンドmeetによりあるペティションを指定する。プレイス31は、ペティションにより指定された条件に該当するエージェントを探す。そして、プレイス31内に該当するエージェントがなければ、そのようなエージェントが入ってくるまで待つ。

【0045】プレイス31内のエージェント33がペティションの条件に該当すれば、プレイス31は、エージェント32が相互作用を希望していることをエージェント33に伝える。そして、エージェント33がエージェント32の希望を受け入れる旨の戻り値を返すと、プレイス31は、エージェント33へのポインタをmeetの戻り値としてエージェント32に返す。その後、エージェント32は、エージェント33へ直接アクセスして、情報交換等を行うことが可能になる。

【0046】図7は、上述のようなリモートプログラミングの手法を図2のネットワークの経路制御に適用した場合の各ルータの概略構成を示している。図7のルータは、制御エージェント部41、通信ポート制御部42、

および通信ポート部43を備える。

【0047】通信ポート制御部42は、通信に必要な経路表を作成・保持し、通信ポート部の制御を行う。通信ポート部43は、通信ポート制御部42や制御エージェント部41からの指示で、通信ポートを制御し、データフローのモニタ等を行う。例えば、通信ポート制御部42からは、通信を遮断するためのフィルタ設定やポートのモニタ等の指示が通信ポート部43に送られ、通信ポート部43は設定結果やフィルタ情報などが返される。

【0048】制御エージェント部41は、管理者に代わってネットワークの通信経路を制御する制御プロセスである制御エージェントを生成し、適当なプレイス内で動作させる。制御エージェントはネットワーク上の他の機器に移動して、コマンドmeetによりその機器内の制御エージェントと情報を交換することができる。制御エージェント部41は、ネットワーク上で経路情報を保持・配付するゲートウェイ機器や末端のハブのような、各ネットワーク機器上に実装される。

【0049】制御エージェントの具体的な動作内容は次の通りである。

(1) 障害時の迂回通信路（代替経路）の作成など、通信路の経路制御が基本動作である。このような場合、通信ポート制御部42や通信ポート部43の制御を行う。具体的には、通信ポート制御部42に初期化や経路情報の設定等の指示を与え、設定結果や経路情報等を受け取る。また、通信ポート部43にフィルタ設定やモニタ等の指示を与え、設定結果やフィルタ情報等を受け取る。

(2) 通常時は、通信路をモニタして負荷状況をチェックしたり、定期的に他の通信機器の制御エージェントと通信を行って、緊急連絡表と呼ばれる緊急時の優先通信先アドレスを納めた表を保持・更新する。

(3) 通信路が一度断たれた場合、管理者による誤接続や第三者による詐称接続を防ぐため、通信路が再び接続される時に、他の制御エージェントとの間で互いの機器の認証を行う。そして、認証確認後に通信路を復旧する。

【0050】制御エージェント部41は、通信ポート制御部42や通信ポート部43が障害を起こした場合にも他の機器との連絡を行うことができるように、これらとはハードウェア的に独立していることが望ましい。

【0051】次に、図8から図10までを参照しながら、制御エージェント部41、通信ポート制御部42、および通信ポート部43が保持するデータの内容について説明する。これらのデータの使用方法については後述することにする。

【0052】図8は、制御エージェント部41内に保持される緊急連絡表、制御エージェント自己情報、および認証用復号鍵のデータ構造を示している。緊急連絡表は、送信対象の数だけリスト形式で作成され、送信対象ルータのアドレス、送信対象ルータ用暗号鍵、対象フラ

グを含む。

【0053】緊急連絡表は、自ルータに障害が発生した場合、そのルータから中継回数が最小で到達できるルータのアドレスを、送信対象ルータのアドレスとして格納する。実際には、自ルータと同じネットに属している他のルータまでの中継回数が最小であるはずなので、それらが通知すべき送信対象ルータとなる。

【0054】つまり、同じネットに属するルータは互いのアドレスを、緊急連絡用の通知先として持ち合っていることになる。代替経路を設定する候補となるルータは、これらの送信対象ルータから選ばれる。これにより、障害発生時にも、迅速に代替経路を探索することが可能になる。

【0055】対象フラグは、主として復旧時の通知先を管理するために用いられる。最初に障害情報が送信対象ルータに送られると、対象フラグには「送信」のようなデータが格納される。

【0056】制御エージェント自己情報は、自ルータのアドレス、自ルータの最新の経路表の情報、自ルータ宛送信に相手が必要とする暗号鍵、制御エージェント状態フラグを含む。制御エージェントは、この自己情報を持ってネットワーク上を移動することができる。状態フラグには、「通知」、「完了」、「不正」のように、制御エージェントの処理の状態を表すデータが格納される。

【0057】また、認証用復号鍵としては、自ルータでの認証時に必要な復号鍵が格納される。図9は、通信ポート制御部42内に保持される経路表のデータ構造を示している。経路表は、送信先を表す送信アドレス（送信先アドレス）、送信アドレスへの経路となるルータのアドレス（送信先ルータアドレス）、送信アドレスへの中継回数、代替フラグ、代替依頼を行ったルータのアドレス（代替依頼ルータアドレス）を含む。代替フラグには、「通常」、「代替」、「元」のように、送信先ルータの役割を表すデータが格納される。

【0058】図10は、通信ポート部43内に保持されるデータの構造を示している。通信ポート部43は、通信ポート番号、現在設定されている遮断フィルタの種類などの制御情報、識別フラグを保持する。

【0059】図11は、図7のルータのシステム構成例を示している。図11のルータは、処理装置51、55、通信ポート58、およびそれらを結合するバス54を備え、通信ポート58により通信ネットワーク59に接続している。ここで、通信ネットワーク59は、例えば図2のネット1、ネット2、ネット3、ネット4等に相当する。

【0060】処理装置51は、CPU（中央処理装置）52およびメモリ53を備え、メモリ53を利用してプログラムを実行することにより制御エージェントを生成して、制御エージェント部41の機能を実現する。

【0061】また、処理装置55は、CPU56および

メモリ57を備え、メモリ57を利用してプログラムを実行することにより、通信ポート制御部42および通信ポート部43の機能を実現する。

【0062】このように、制御エージェント部41を通信ポート制御部42および通信ポート部43からハード的に独立させることにより、ルータ本体が故障してしまっても、制御エージェントを正しく動作させることが可能になる。

【0063】次に、図12から図19までを参照しながら、ルータ4が不調になったときの経路制御処理および復旧処理について詳細に説明する。図12はルータ4に異常が発生する前の各ルータ内の経路表を示しており、図13は異常発生後の各ルータ内の経路表を示している。また、図14から図19までは、各ルータの制御エージェントの処理フローを示している。

【0064】図14は、異常になったルータ4の通信ポート制御部42と制御エージェントの処理のフローチャートである。図14において処理が開始されると、通信ポート制御部42は、ルータが不調となったことで、自ルータ上にある制御エージェント部41に「異常」という通知を伝えて（ステップS1）、処理を終了する。

【0065】制御エージェント部41の制御エージェントは、通信ポート制御部42からの信号を定期的に見張っていて、この異常通知を捉える（ステップS2）。次に、管理用通信プロトコル、および制御エージェント自身が通信に用いる通信ポート以外をフィルタ（遮蔽）するように、通信ポート部43に指示する（ステップS3）。

【0066】これにより、このルータ4は通常の通信ルートから隔離される。このとき、通信ポート部43は、フィルタしたポートの識別フラグ（図10参照）に、『ルータ4』と設定する。

【0067】次に、制御エージェントは、自ルータ異常時の代替経路の候補になるような他のルータを調べるため、制御エージェント部41内に格納されている図8のような緊急連絡表を検索する（ステップS4）。そして、異常を通知すべき対象ルータが登録されているかどうかを調べる（ステップS5）。

【0068】この例では、ルータ4が接続されているネット2に属するルータ1とルータ3、およびネット3に属するルータ2が送信対象として緊急連絡表に登録されている。したがって、通知すべきルータが緊急経路表に見つかったので、制御エージェントはコマンドsendを実行し、送信対象ルータの数だけ自己の複製を作成する（ステップS6）。このとき、制御エージェント自己情報も同時にコピーされる。

【0069】sendは、エージェントの手続きliveの中で実行され、そのエージェントの複製を作って他のプレイスに送るコマンドである。ここでは、sendの実行により、ステップS6、S7、S8の処理が行わ

れる。

【0070】制御エージェントは、作成した複数エージェントの自己情報の状態フラグを『通知』に設定する（ステップS7）。このとき、通知先のルータ別に暗号鍵を使って、複数エージェントを暗号化しておく。次に、送信対象ルータ（この例ではルータ1～3）に複製エージェントを送り、同時に緊急連絡表の対象フラグを『送信』に設定する（ステップS8）。

【0071】送り元であるルータ4の制御エージェントは待機手続きを行い（ステップS9）、送った複製エージェントがすべて戻ってくるまで待機状態になる。もし、複製エージェントが戻ってこない場合は、例外処理として、管理者に通知する、再送する、エラーで停止するなどの何等かの処理を行う。

【0072】図15は、ステップS9で行われる制御エージェントの待機手続きのフローチャートである。図15において処理が開始されると、制御エージェントは、戻ってきた各々の複製エージェントについて、図16のような認証手続きを行う（ステップS21）。

【0073】図16において処理が開始されると、制御エージェントは、他のルータから送り返されてきたエージェントを自分が保有する復号鍵で復号する（ステップS31）。次に、そのエージェントの自己情報内の自ルータのアドレスを、緊急連絡表に持っている送信対象ルータのアドレスと比較して（ステップS32）、処理を終了する。

【0074】次に、図15のステップS22において、やって来たエージェントが持つアドレスが正しいかどうか認証する。戻ってきた複製エージェントが持つアドレスは、送信時に送信元のルータのアドレスに書き換えられているため、緊急連絡表内の送信対象ルータのいずれかのアドレスと一致するはずである。

【0075】送信対象ルータのアドレスに一致すれば、それを正しいアドレスと判定し、受信エージェント数のカウンタ値に1を加える（ステップS23）。そして、カウンタ値が送信した複製エージェントの数に達したかどうかを判定し（ステップS24）、それに達すれば処理を終了する。

【0076】ステップS22においてアドレスが一致しない場合、およびステップS24においてカウンタ値が送信した複製エージェントの数に達しない場合は、ステップS21以降の処理を繰り返す。

【0077】すべての複数エージェントが戻ってきたことが確認されると、次に、それらの状態フラグを調べる（ステップS10）。そして、状態フラグが『経路外』で戻ってきた場合は、緊急連絡表の対応する送信対象ルータの対象フラグにある『送信』の設定を解除する。これは、その送信対象ルータが代替経路として使用できないことを意味している。

【0078】また、状態フラグが『不正』で戻ってきた

場合は、例外処理として、管理者に通知する、再送する、エラーで停止するなどの何等かの処理を行う。代替経路が設定されたルータからの複数エージェントは、状態フラグが『完了』となって戻ってくる。

【0079】こうして、送信した複数エージェントが戻ってくるにより、いくつかのルータ上で代替経路が設定されたことが分かるので、管理者に作業開始の指示を与え（ステップS10）、処理を終了する。その後、管理者は不調となったルータ4の復旧作業を行う。ステップS5において、緊急連絡表に通知先のルータが登録されていない場合は、直ちにステップS11の処理を行って、処理を終了する。

【0080】図17は、ルータ4から複数エージェントを受け取った正常なルータの制御エージェントの処理のフローチャートである。この例では、ルータ1、ルータ2、ルータ3がこの処理を行う。図17において処理が開始されると、ルータ1～3の制御エージェントは、まず送られてきたエージェントの認証手続きを行う（ステップS41）。

【0081】ここで、送られてきたエージェントを復号し（図16、ステップS31）、自ルータが緊急連絡表に持つ送信対象ルータのアドレスと、送られてきたエージェントが持つアドレスを比較する（ステップS32）。そして、それが正しい送信元からの複製エージェントかどうか認証する（ステップS42）。

【0082】ルータ4のアドレスは、ルータ1～3の緊急連絡表に登録されているはずなので、そこから送られてきた複製エージェントは正しいエージェントとして認証される。

【0083】送られてきたエージェントのアドレスが正しくなければ、その状態フラグを『不正』に設定して（ステップS52）、送信元のルータに送り返し（ステップS51）、処理を終了する。あるいは、ステップS52において例外処理を行ってもよい。

【0084】送られてきたエージェントのアドレスが正しければ、次に、自分のいるルータの通信ポート制御部42にある経路表から、その複製エージェントが持っているルータ4のアドレスが含まれる経路を探す。そして、その代替フラグを『元』に設定する（ステップS43）。

【0085】例えば、図12のルータ2の経路表には、ネット2へ送信するときの送信先ルータはルータ4であることが記載されているので、その経路の代替フラグを、図13に示されるように『元』に設定する。これは、ルータ4に異常が発生したため、その経路が使えなくなったことを意味する。

【0086】次に、自ルータの経路表を更新するように、通信ポート制御部42に指示する（ステップS44）。これにより、通信ポート制御部42が同じネットに属する他のルータと経路情報をやり取りし、不調とな

ったルータ4以外の送信先ルータを求めて、経路表を更新する。ただし、この更新処理において、代替フラグが『通常』以外の値に設定されている経路の削除等は行わないものとする。

【0087】次に、ルータ4から来た複製エージェントから、その自己情報に含まれるルータ4の最新の経路表を受け取り（ステップS45）、それを検索して（ステップS46）、その経路表にある送信先アドレスが自ルータの経路表の送信先アドレスにあるかどうかを調べる（ステップS47）。

【0088】ルータ4の送信先アドレスが自ルータの経路表になければ、自ルータは代替経路にはならないので、ルータ4から来た複製エージェントの状態フラグを『経路外』に設定する（ステップS47）。そして、ルータ4向けの暗号鍵で暗号化してルータ4に送り返し（ステップS51）、処理を終了する。

【0089】ルータ4の送信先アドレスが自ルータの経路表にあれば、その経路の代替フラグを『代替』に設定する。これにより、複製エージェントを受け取ったルータを含む特定の経路が、自動的に代替経路に設定される。

【0090】例えば、ルータ2の経路表には、更新処理により通信ポート制御部42がルータ5と経路情報のやり取りをした結果、図13に示すように、ネット2へ送信するときの送信先ルータをルータ5とする経路情報が新たに加わっている。そこで、その経路の代替フラグを『代替』に設定する。

【0091】次に、その経路の「代替依頼を行ったルータのアドレス」として、複製エージェントを送ってきたルータ4のアドレスを設定する（ステップS49）。ここでは、ルータ2の経路表の代替フラグが『代替』となっている経路に、代替依頼ルータアドレスとしてルータ4のアドレスが設定される。

【0092】次に、ルータ4から来た複製エージェントの状態フラグを『完了』に設定し、ルータ4向けの暗号鍵で暗号化して（ステップS50）、ルータ4に送り返し（ステップS51）、処理を終了する。こうして、代替経路の設定が完了する。

【0093】図12のルータ1およびルータ3の経路表もルータ2と同様にして更新され、代替フラグ等が書き換えられて、図13に示す経路表のようになる。これにより、ワークステーション11==ネット3==ルータ2==ネット4==ルータ5==ネット1==ルータ3==ネット2==ルータ1==メインフレーム13のような代替経路が設定される。

【0094】尚、図13において、ルータ4から複製エージェントの送付を受けなかったルータ5の経路表は変更されていない。ルータ1、ルータ2、ルータ3から『完了』の状態フラグを持つ複製エージェントがルータ4に戻ると、管理者がルータ4の修理等の作業を行う。

作業が終了すると、管理者は各ルータの制御エージェントに復旧時の処理を指示する。

【0095】図18は、ルータ4上の制御エージェントの復旧時の処理のフローチャートである。図18において処理が開始されると、制御エージェントは、まず自己情報として保持している異常前の経路表を通信ポート制御部42に設定する(ステップS61)。このとき、通信ポート部43はまだフィルタされているので、他の代替ルータに回っているパケットの経路を乱すことはない。

【0096】次に、緊急連絡表を参照して、復旧を通知すべきルータがあるかどうかを判定する(ステップS62)。緊急連絡表内の対象フラグが『送信』に設定されている送信対象ルータが、通知すべきルータとなる。

【0097】通知すべきルータがなければ、通信ポート58に設定したフィルタのうち、図10の識別フラグが『ルータ4』に設定されているフィルタを解除するように通信ポート部43に指示して(ステップS67)、処理を終了する。

【0098】通知すべきルータがあれば、コマンドsendを実行して、ステップS63、S64、S65の処理を行う。まず、通知対象ルータの数だけ自己の複製を作成し(ステップS63)、作成した複数エージェントの状態フラグを『通知』に設定する(ステップS64)。このとき、通知先のルータ別に暗号鍵を使って、複数エージェントを暗号化する。

【0099】次に、通知対象ルータ(この例ではルータ1～3)に複製エージェントを送り(ステップS65)、図15のような待機手続きを行って、送った複製エージェントがすべて戻ってくるまで待機状態になる(ステップS66)。もし、複製エージェントが戻ってこない場合は、何等かの例外処理を行う。

【0100】複製エージェントが戻ってくると、各々について図16のような認証手続きを行う(ステップS21)。状態フラグが『不正』に戻ってきた場合は、何等かの例外処理を行う。

【0101】すべての複製エージェントが戻ってきたら、次に、識別フラグが『ルータ4』に設定されているフィルタを解除するように通信ポート部43に指示し(ステップS67)、処理を終了する。

【0102】こうして、ルータ4の通信ポート58のフィルタが解除され、ルータ4は正常状態に復帰する。図19は、複製エージェントを受け取ったルータ1、ルータ2、ルータ3上の制御エージェントの復旧時の処理のフローチャートである。図19において処理が開始されると、制御エージェントは、まず図16のような認証手続きを行って(ステップS71)、送られてきた複製エージェントを復号し(ステップS31)、自ルータが緊急連絡表に持つ送信対象ルータのアドレスと、送られてきたエージェントが持つアドレスを比較する(ステップ

S32)。そして、それが正しい送信元からの複製エージェントかどうか認証する(ステップS72)。

【0103】送られてきたエージェントのアドレスが正しくなければ、その状態フラグを『不正』に設定して(ステップS77)、送信元のルータに送り返し(ステップS76)、処理を終了する。あるいは、ステップS77において例外処理を行ってもよい。

【0104】送られてきたエージェントのアドレスが正しければ、次に、自分のいるルータの通信ポート制御部42にある経路表内で、『元』に設定されている代替フラグを『通常』に再設定する(ステップS73)。例えば、図13のルータ2の経路表には、ルータ4経由のネット2への送信経路の代替フラグが『元』に設定されているので、これを『通常』に再設定する。

【0105】次に、自ルータの経路表内で、代替フラグが『代替』に設定されている経路を削除する。例えば、ルータ2の経路表には、ルータ5経由のネット2への送信経路の代替フラグが『代替』に設定されているので、この経路を経路表から削除する。

【0106】次に、ルータ4から来た複製エージェントの状態フラグを『完了』に設定し、ルータ4向けの暗号鍵で暗号化する(ステップS75)。そして、それをルータ4に送り返して(ステップS76)、処理を終了する。

【0107】図13のルータ1およびルータ3の経路表もルータ2と同様にして書き換えられ、図12のような異常発生前の経路表に復帰する。この結果、ルータ4を経由するワークステーション11==ネット3==ルータ4==ネット2==ルータ1==メインフレーム13の経路が再び利用可能となる。

【0108】本実施形態において、通信経路を変更、あるいは切り替える際、その瞬間の経路上のデータを保証する必要がある。幸い、経路制御が必要となるパケット単位やセル単位での通信では、現在用いられている通信プロトコルに「通信失敗時の再送」という技術が基本的に備えられており、これにより通信データの整合性が保証されている。

【0109】本実施形態を用いた場合でも、時間的に零時間で経路を切り替えることは不可能なので、ある程度は再送パケットが出るのが予想される。しかし、制御エージェントにより積極的に経路の切り替えを制御することで、再送パケットの数は従来の方法よりかなり減少することが期待できる。

【0110】また、本実施形態においては、RIP等の従来の経路制御プロトコルをそのまま活用できるため、比較的簡単に経路制御装置を実現することができる。以上のようなリモートプログラミングを用いた実施形態によれば、制御エージェントの自律性を利用することにより、ネットワーク上の各機器が自主的に異常を発見して、代替経路を確保する。したがって、管理者は代替経

路の設定等の作業を省略して、異常機器の復旧作業に専念することができる。

【0111】尚、本実施形態においてはルータが経路制御装置の機能を持っているが、これに限らず、経路制御装置をネットワーク上の任意の機器内に設けることが可能である。また、ネットワークの接続形態は図2のものに限られず、任意の形態を取ることができる。

【0112】また、異常発生時に作成された複製エージェントは、送信先のルータ上で代替ルータを発見できなければ、それを発見できるまで自己複製を繰り返すようにしてもよい。この場合、各送信先のルータの緊急連絡表を参照して、その送信対象ルータの数だけの複製エージェントをさらに作成することになる。

【0113】また、本発明を実施する際に必ずしもエージェントを用いる必要はなく、それぞれの制御エージェントの処理を普通のプロセスにより行ってもよい。この場合は、ネットワークを介したやり取りは、例えばRPC (remote procedure call) 等により実行される。

【0114】本発明の他の適用例としては、次のようなものがある。

〔1〕通信ネットワークのセキュリティを守るためのファイアウォール（防火壁）の構築

通信路をモニタ中にアクセス禁止先への通信を発見した場合、その通信に対する通信路を動的にフィルタするなど。

〔2〕商用通信ネットワークのトラフィック集中時間における回線制御

回線の負荷に応じて、通信を流す通信路を増やしたり、他の通信を一時抑制するなど。

〔3〕混雑時や災害時における交通路などの制御
通信経路を制御する代わりに、人や物資などが流れる経路を制御する。例えば、ネットワーク状に配置された交通路上で信号機制御などを行って、渋滞（輻湊）時の交通量を調整する。

【0115】

【発明の効果】本発明によれば、ネットワーク状に構成された通信路や交通路等の経路を動的に制御して、障害発生時の代替経路を自律的に確保することができる。したがって、ネットワークが一時的に高負荷になった場合や、ネットワークそのものがダウンした場合などに、ネットワーク自身が自動的に迂回経路を設定できる。

【0116】このため、管理者はネットワークの状況を調べて代替経路を設定する必要がなく、また、ある機器が不調になった時の代替経路をあらかじめ登録しておく必要もない。

【図面の簡単な説明】

【図1】本発明の原理図である。

【図2】コンピュータ・ネットワークを示す図である。

【図3】プレイスの構成を示す図である。

【図4】エージェントの構成を示す図である。

【図5】オペレーションgoを示す図である。

【図6】オペレーションmeetを示す図である。

【図7】ルータの概略構成図である。

【図8】制御エージェント部内のデータ構造を示す図である。

【図9】通信ポート制御部内のデータ構造を示す図である。

【図10】通信ポート部内のデータ構造を示す図である。

【図11】ルータのシステム構成図である。

【図12】異常発生前の経路表を示す図である。

【図13】異常発生後の経路表を示す図である。

【図14】異常ルータの処理のフローチャートである。

【図15】制御エージェントの待機手続きのフローチャートである。

【図16】制御エージェントの認証手続きのフローチャートである。

【図17】正常ルータの処理のフローチャートである。

【図18】復旧時における異常ルータの処理のフローチャートである。

【図19】復旧時における正常ルータの処理のフローチャートである。

【符号の説明】

1, 4 情報処理装置

2 検出手段

3 指示手段

5 受信手段

6 探索手段

7 記憶手段

11 ワークステーション

12 管理サーバ

13 メインフレーム

21, 24, 31 プレイス

22, 32, 33 エージェント

23 チケット

41 制御エージェント部

42 通信ポート制御部

43 通信ポート部

51, 55 処理装置

52, 56 CPU

53, 57 メモリ

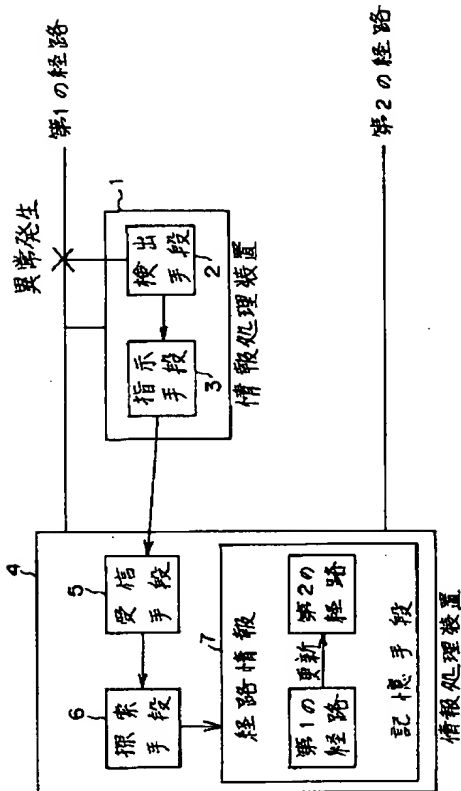
54 バス

58 通信ポート

59 通信ネットワーク

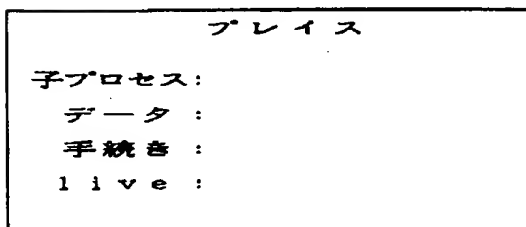
【図1】

本発明の原理図



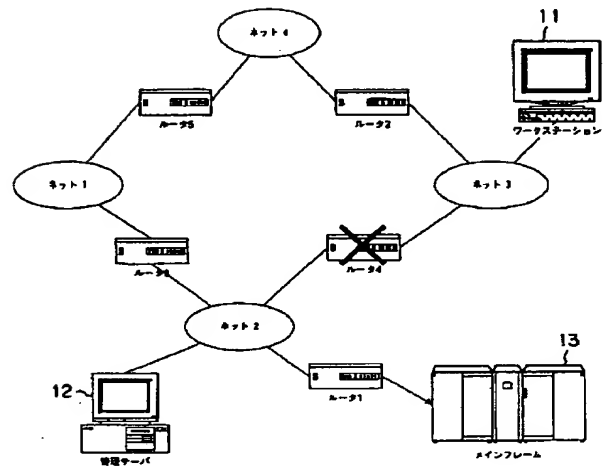
【図3】

プレイスの構成を示す図



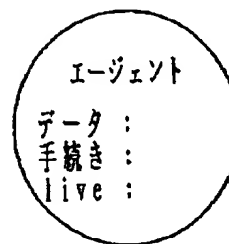
【図2】

コンピュータ・ネットワークを示す図



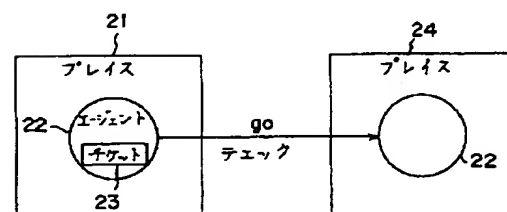
【図4】

エージェントの構成を示す図



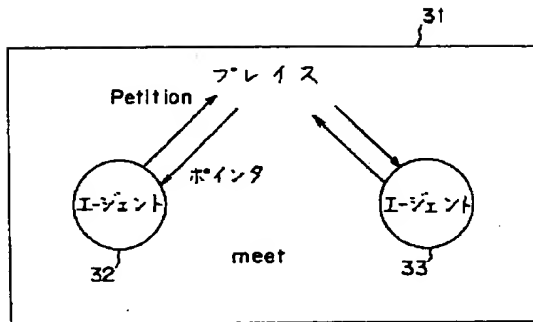
【図5】

オペレーション go を示す図



【図6】

オペレーション meet を示す図



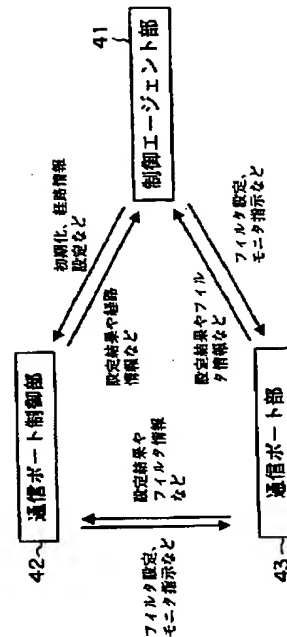
【図10】

通信ポート部内のデータ構造を示す図

通信ポート番号	現在設定されている制御情報 (遠征フィルタの種類など)	識別フラグ
---------	--------------------------------	-------

【図7】

ルータの概略構成図



【図8】

制御エージェント部内のデータ構造を示す図

- ・ 緊急連絡表（送信対象の数だけリスト形式で保持）

送信対象ルータのアドレス	送信対象ルータ用暗号鍵	対象フラグ
--------------	-------------	-------

- ・ 制御エージェント自己情報

自ルータのアドレス	自ルータの最新の経路表	自ルータ宛送信に相手が必要とする暗号鍵	制御エージェント状態フラグ
-----------	-------------	---------------------	---------------

- ・ 認証用復号鍵

自ルータでの認証時に必要な復号鍵

【図9】

通信ポート制御部内のデータ構造を示す図

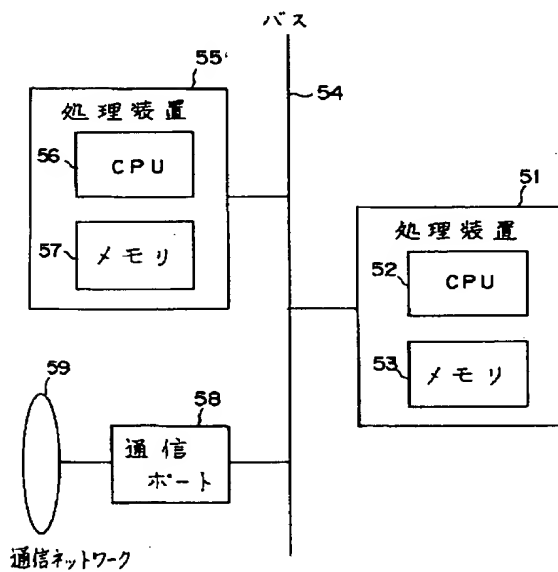
経路表

送信アドレス	送信アドレスへの経路となるルータのアドレス	送信アドレスへの中継回数	代替フラグ	代替依頼を行ったルータのアドレス
--------	-----------------------	--------------	-------	------------------

【図11】

【図12】

ルータのシステム構成図



【図16】

異常発生前の経路表を示す図

ルータ1（ルータ4異常前）

送信先アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替依頼ルータアドレス
メインフレーム	なし	0	通常	なし
ネット2	なし	0	通常	なし
ネット3	ルータ4	1	通常	なし
ネット1	ルータ3	1	通常	なし

ルータ2（ルータ4異常前）

送信先アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替依頼ルータアドレス
ネット3	なし	0	通常	なし
ネット4	なし	0	通常	なし
ワークステーション	なし	0	通常	なし
ネット1	ルータ5	1	通常	なし
ネット2	ルータ4	1	通常	なし

ルータ3（ルータ4異常前）

送信先アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替依頼ルータアドレス
ネット1	なし	0	通常	なし
ネット2	なし	0	通常	なし
ネット3	ルータ4	1	通常	なし
ネット4	ルータ5	1	通常	なし

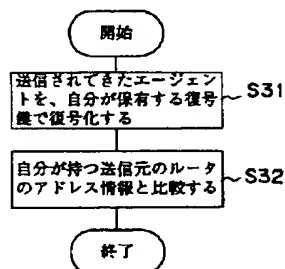
ルータ5（ルータ4異常前）

送信先アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替依頼ルータアドレス
ネット1	なし	0	通常	なし
ネット4	なし	0	通常	なし
ネット2	ルータ3	1	通常	なし
ネット3	ルータ2	1	通常	なし
ワークステーション	ルータ2	1	通常	なし

ルータ4（異常前）

送信先アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替依頼ルータアドレス
ネット2	なし	0	通常	なし
ネット3	なし	0	通常	なし
ワークステーション	なし	0	通常	なし
メインフレーム	ルータ3	1	通常	なし
ネット1	ルータ2	1	通常	なし
ネット4	ルータ1	1	通常	なし

制御エージェントの認証手続きのフローチャート



【図13】

異常発生後の経路表を示す図

ルータ1 (ルータ4異常後)				
送信元アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替先ルータアドレス
ダイクレーン	なし	0	通常	なし
ネット2	なし	0	通常	なし
ネット1	ルータ3	1	通常	なし
ネット3	ルータ3	3	代替	ルータ4
ネット3	ルータ4	1	元	なし

ルータ2 (ルータ4異常後)				
送信元アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替先ルータアドレス
ネット3	なし	0	通常	なし
ネット4	なし	0	通常	なし
ワークステーション	ルータ5	1	通常	なし
ネット1	ルータ5	1	通常	なし
ネット2	ルータ5	2	代替	ルータ4
ネット2	ルータ5	2	元	なし

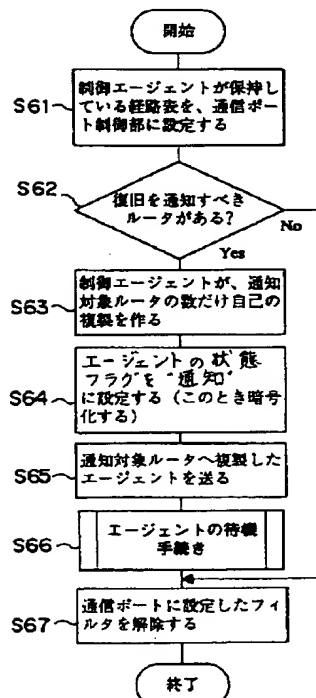
ルータ3 (ルータ4異常後)				
送信元アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替先ルータアドレス
ネット1	なし	0	通常	なし
ネット2	なし	0	通常	なし
ネット3	ルータ4	1	元	なし
ネット3	ルータ5	2	代替	ルータ4
ネット4	ルータ5	1	通常	なし

ルータ5 (ルータ4異常後)				
送信元アドレス	送信先ルータアドレス	中継回数	代替フラグ	代替先ルータアドレス
ネット1	なし	0	通常	なし
ネット4	なし	0	通常	なし
ネット2	ルータ3	1	通常	なし
ネット3	ルータ2	1	通常	なし
ワークステーション	ルータ2	1	通常	なし

【図18】

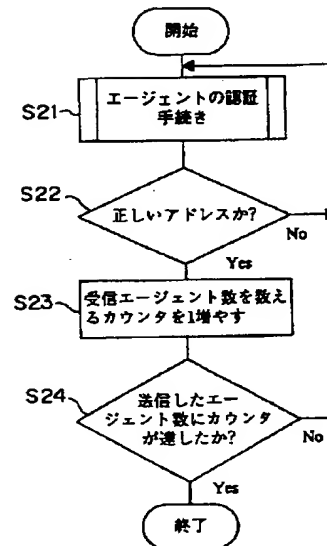
復旧時における異常ルータの処理のフローチャート

制御エージェント



【図15】

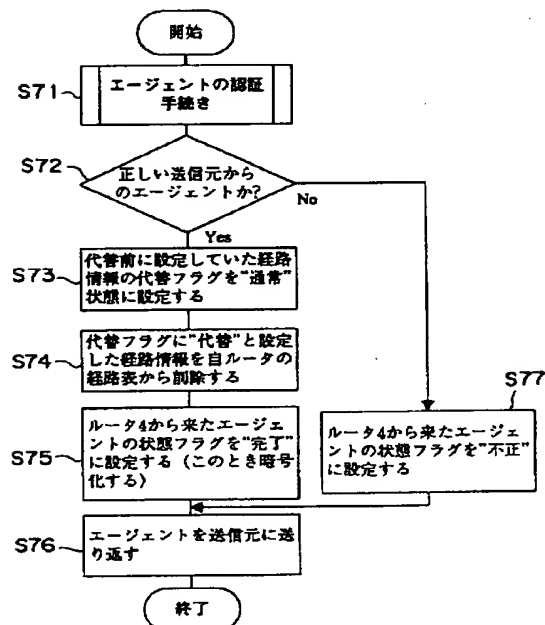
制御エージェントの待機手続きのフローチャート



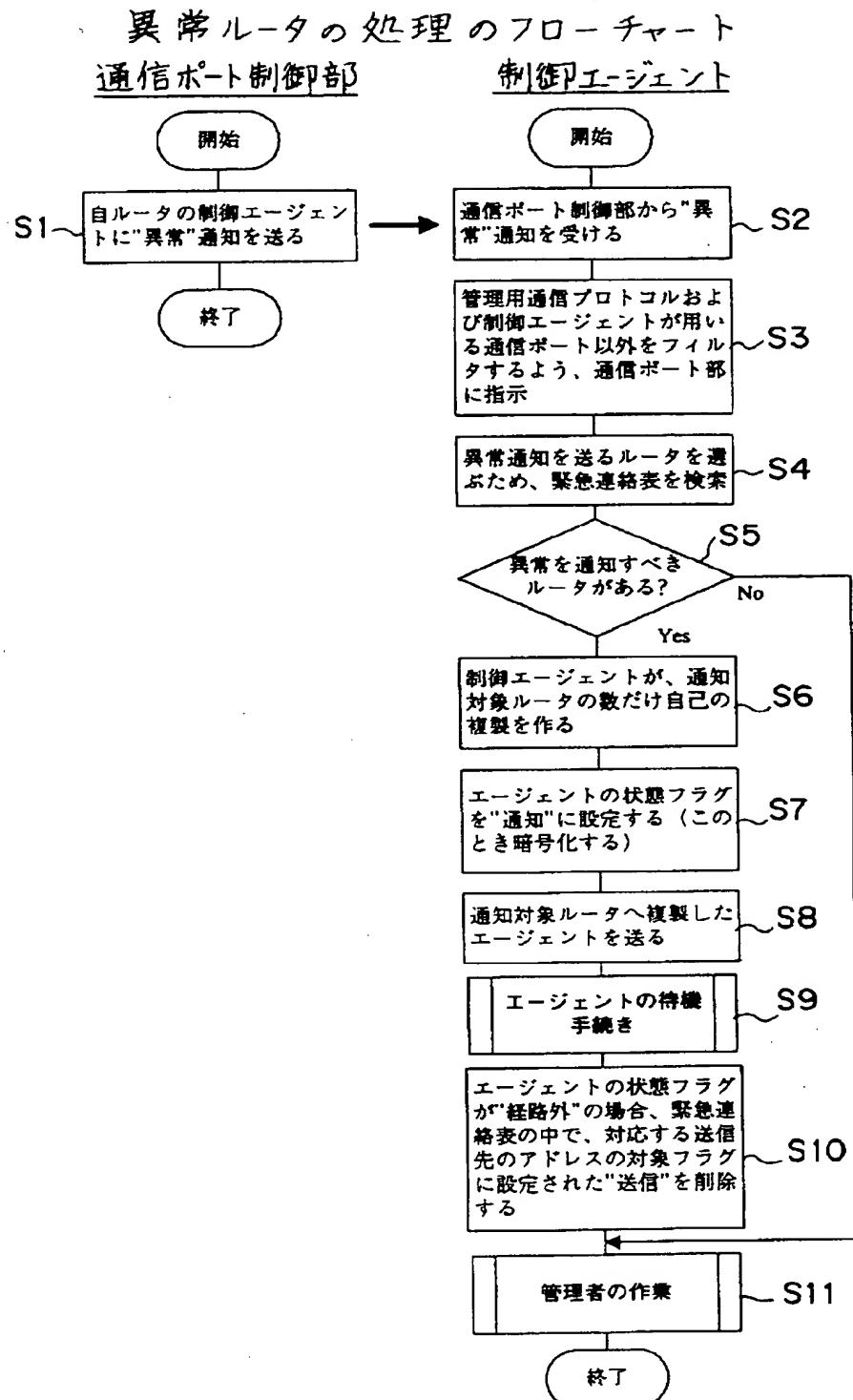
【図19】

復旧時における正常ルータの処理のフローチャート

制御エージェント



【図14】



【図17】

正常ルータの処理のフローチャート
制御エージェント

